A New Network Security Architecture Based on SDN / NFV Technology

Zhu Lina
Network Information Security Department
Guangdong Police College
Guangzhou, China

Zhu Dongzhao
Heilongjiang Branch
China Mobile Information Technology co., LTD
Harbin, China

***Abstract*— The new network based on software-defined network SDN and network function virtualization NFV will replace the traditional network, so it is urgent to study the network security architecture based on the new network environment. This paper presents a software - defined security SDS architecture. It is open and universal. It provides an open interface for security services, security devices, and security management. It enables different network security vendors to deploy security products and security solutions. It can realize the deployment, arrangement and customization of virtual security function VSFs. It implements fine-grained data flow control and security policy management. The author analyzes the different types of attacks that different parts of the system are vulnerable to. The defender can disable the network attacks by changing the server-side security configuration scheme. The future research direction of network security is put forward.**

Keywords- Software Defined Network, Network Function Virtualization, Software Defined Security, Virtual Security Function, Security Service Function Path

I. INTRODUCTION

We are in an era of network transformation. In front of the explosive growth of traffic and application demand, the traditional network has been overwhelmed. Network virtualization, software definition and cloud are the direction of current network transformation, and are also ready for the arrival of 5G. The new network is based on Software Defined Network (SDN) and Network Functions Virtualization (NFV). Software defined network (SDN) separates the control layer and data layer of network equipments. The network can not only complete the task of data transmission, but also become a kind of flexible resource that can be deployed as the computing and storage resources after being virtualized. It is no longer the bottleneck that restricts the online business and cloud efficiency. Network function Virtualization (NFV) decouples software and hardware, so that network device functions no longer depend on special hardware. Virtualization technology and function abstraction realize network function software, rapid development and deployment of new business, automatic deployment, elastic scaling, fault isolation and self-healing based on actual business requirements[1].

In the new network environment of virtualization, automation, software and dynamic, the old unchanged security mechanism and security policy deployment will not be appropriate, so it is urgent to study the network security architecture based on the new network environment. Due to the flexible and definable characteristics of SDN and NFV, researchers are discussing how to use software defined security (SDS) to solve the security problems in the new network environment. At present, many security companies at home and abroad have put forward their own software defined security (SDS) solutions: H3C company innovatively integrates NFV Manager into control cluster in the form of APP in the control plane of software defined network (SDN).For the first time, embedded security virtual switch is installed in the basic hardware layer and physical abstraction layer, forming a state-based security protection system[2]. In 2015, Lvmeng Technology Co., Ltd. released the "2015 Lvmeng technology software definition security SDS white paper" and the "smart security" strategy.At present, the company's software definition security system supports apt, cloud web security, adaptive access control, situation awareness and other security applications in the mixed information technology environment[3]. Huawei's SNC controller can provide end-to-end full scenario solutions to help operators quickly deploy SDN networks, reduce OPEX, rapidly deploy new services and accelerate business innovation. Huawei's SNC controller can provide end-to-end full scenario solutions to help operators quickly deploy SDN networks, reduce OPEX, rapidly deploy new services and accelerate business innovation. In the SNC controller, the compatibility, interworking and upgrading of the existing network are fully considered, so that the operator network can smoothly transit to the SDN network architecture [4].

At present, the proposed closed system is still a single security product and solution, which does not provide open interfaces in security equipment, security services, security management, control capabilities and other aspects. Some schemes mainly focus on security management and lack intelligence threat analysis and processing. The malicious attacks can not be detected and blocked in time. The user-defined business details and business requirements are not supported. The real customized products cannot be provided, and the detection and deep data mining mechanism cannot find the real threats.

This paper proposes a standard, open-source and user-defined technology innovation, which provides a coordinated, interoperable and controllable security platform for many security products and service providers, and a reference architecture and blueprint for software definition security.

978-1-7281-5904-1/20/$31.00 ©2020 IEEE
DOI 10.1109/ICCEA50009.2020.00146

II. DESIGN OF SOFTWARE DEFINITION SECURITY (SDS) ARCHITECTURE BASED ON SDN / NFV TECHNOLOGY

A. *Basic framework*

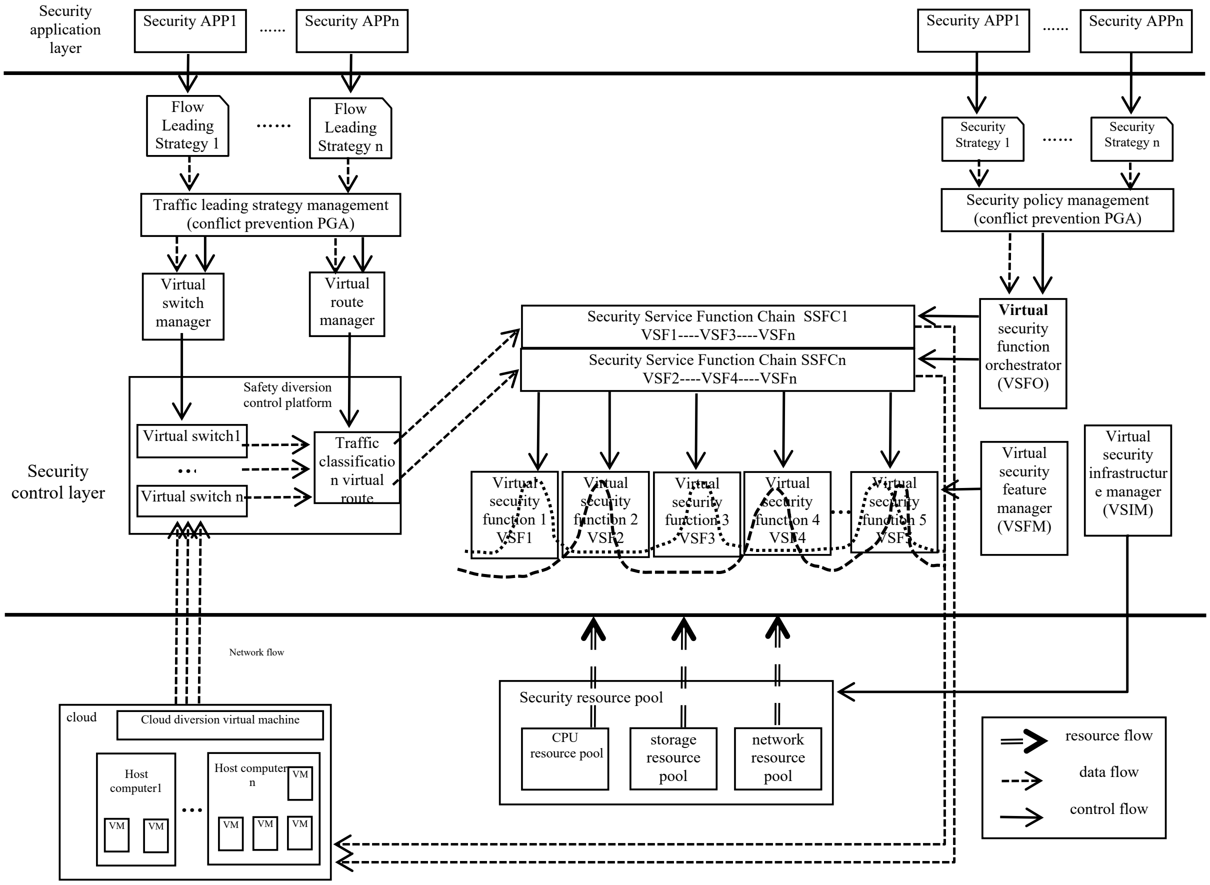
Security application layer
Security APP1
......
Security APPn
Flow Leading Strategy 1
......
Flow Leading Strategy n
Traffic leading strategy management (conflict prevention PGA)
Virtual switch manager
Virtual route manager
Safety diversion control platform
Virtual switch1
...
Virtual switch n
Traffic classification virtual route
Security control layer
Security APP1
......
Security APPn
Security Strategy 1
......
Security Strategy n
Security policy management (conflict prevention PGA)
Security Service Function Chain SSFC1
VSF1----VSF3----VSFn
Security Service Function Chain SSFCn
VSF2----VSF4----VSFn
Virtual security function orchestrator (VSFO)
Virtual security function 1 VSF1
Virtual security function 2 VSF2
Virtual security function 3 VSF3
Virtual security function 4 VSF4
Virtual security function 5 VSF5
Virtual security feature manager (VSFM)
Virtual security infrastructure manager (VSIM)
Network flow
cloud
Cloud diversion virtual machine
Host computer1
VM
VM
...
Host computer n
VM
VM
VM
VM
Security resource pool
CPU resource pool
storage resource pool
network resource pool
resource flow
data flow
control flow

Figure 1. SDS basic architecture diagram

B. *Constructing virtual security resource pool based on NFV Technology*

The design idea of NFV is to use the general x86 architecture machine to replace the underlying heterogeneous special equipments. The devices are open and compatible. Then using virtualization technology, the device control plane is running on the server, which provides different functions in the virtual layer and allowing functions to be combined and separated. NFV architecture provides an agile service function model, which can realize dynamic and elastic service delivery requirements, realize the movement of various service functions and application workload in the network, and bind service policies to each subscriber.

Based on the idea of NFV, we separate the hardware of security products from the software and run it in the virtual environment of pooling. Pooling of security resources can provide resources to a variety of virtual network devices (such as virtual network security function, virtual switch, traffic classification virtual router) in the upper layer of network security control layer.The resources of these virtual network devices are dynamically created or reallocated according to the needs of customers, which can meet the elastic expansion of users' security capabilities and meet the security needs flexibly and in real time. Virtualization, software definition security and other technologies improve the utilization efficiency of operating resources and flexible resource management.

C. *Using virtual switch to realize diversion on diversion platform*

Virtual switch is a switch that logically integrates multiple physical connections and is integrated into a virtual platform, and then copied to a physical device using virtualization technology. The virtual interactive machine collects and records the topological relations learned by each member, and realizes the topology management of the whole system. It enhances communication reliability, working efficiency and bandwidth capacity, and realizes load balancing and redundancy through EtherChannel technology.

In virtual environment, network attack and security risk exist not only between the host at the bottom of virtual machine, but also between virtual machines. By using the Diversion virtual machine deployed in the cloud environment, the traffic is exported to the virtual switch in the network security control layer outside the cloud. The diversion virtual machine can realize the virtual switch to pull the network traffic out of the cloud data resource pool under various virtualization environments. According to different security policies, traffic is classified and redirected, which expands the analysis space of traffic.

D. Using virtual router to realize traffic classification

In the traditional network, the traffic classification mark is set in the to domain of IP message or the EXP domain of MPLS message, and the router classifies according to the traffic classification mark. In this SDS system, the virtual routing manager in the network security control layer can design the traffic classification strategy according to the traffic traction strategy issued by the application layer, and then send the traffic classification strategy to the traffic classification virtual router. The traffic classification is used to describe the traffic isolation based on the local policy defined for a certain segment of the network. A set of virtual security functions can be assigned to a traffic class. Realize flexible and scalable flow control of flow classification according to any information segment of the message.

E. Virtual Security Function（VSF）

Virtual security function refers to the security services provided by the network security control layer. The security service can be composed of a single or multiple VSFs. Virtual security function (VSF) is used to describe the network security functions that deal with traffic in some way, such as firewall, intrusion detection system(IDS),Intrusion prevention system (IPS), load balancing. Hardware devices can be used to implement one or more virtual security functions.

F. Security Service Function Chain(SSFC)

Security service function chain is a kind of ability to connect virtual security functions (such as firewall, IDS, agent and intrusion prevention system) in the form of chain, which is used to classify traffic. The security service function chain (SSFC) is used to dynamically select, arrange and link the virtual security functions for traffic control and end-to-end delivery of data packets in the network. According to the needs, the arrangement order of virtual security functions can be sequential or parallel, for example, firewall and IDS can be used in the chain of security functions serially or in parallel. Security service function chain provides an infrastructure (including link logic and APIs). Overlay description language is required to provide network service chain and an end-user application defining these service chains[5].

G. Security Service Function Path(SSFP)

The dependence of SSFC on network topology makes it necessary to introduce SSFP.

Security service application layer requires network security control layer to provide flexible, agile and elastic security function chain, but the logic and network topology of virtual network have certain dependence on the order of security function modules in the security function chain. When the order of the security function modules in the SDS network changes, the physical or logic of the network is required to change accordingly, which is contrary to the design specifications of the Internet Service Providers. Hardware movement may cause network downtime and configuration errors, making the original static services unable to be delivered. For example, in cloud services, different tenants communicate through fast tunnel networks such as VLAN. If the service function (such as firewall or IDS) is put in SSFP, the service delivery will be affected, which also limits the scale, capacity and flexibility of the whole network.In addition, in order to provide high availability based on network topology, in addition to the main service functions, redundant service functions are also needed. However, topology dependency limits the high availability of security function modules.

In order to solve the topology dependence of SSFC in service delivery, security service function path (SSFP) is introduced. SSFP is the logical path of packets / frames from source to target in SSFC after fine-grained policies and operational constraints are applied on SSFP.SSFP is a logical concept. It is abstract at one level. Sometimes SSFP may be the same as SSFC, and sometimes multiple SSFP can be designed according to one SSFC. The advantage of SSFP is that the VSFs module in SSFC can be executed according to granularity strategy and operation constraint without changing the topology of SSFC[6].

H. Network security policy management and traffic traction policy management

The traffic pull strategy specifies how to pull traffic between two endpoints in the cloud network. Traffic traction strategy helps to ensure the best performance, redundancy, authentication and data integrity of the network. Ensuring that these goals are achieved on the security services functional chain (SSFC) is a complex issue.

The essence of SSFC is network policy. Application layer users include network administrators, users or tenants of virtual tenant network. They use security applications to generate their own dynamic network security policies, but different policies will inevitably produce policy conflicts.

1) Conflict classification

Set flow table f to include rule sets$\{r_1,r_2,r_3,\ldots\ldots r_i\ldots\ldots r_j\ldots\ldots\}$

We use tuples (n_i,ρ_i,a_i) to represent flow rules r_i showed in TABLE Ⅰ.

TABLE I. FLOW RULES

redundancy	Address Space $n_i \subseteq n_j$; Agreement $\rho_i = \rho_j$; Action $a_i = a_j$
shelter	Priority $p_i < p_j$; Address Space $n_i \subseteq n_j$; Agreement $\rho_i = \rho_j$; Action $a_i \neq a_j$

generalization	Priority $p_i < p_j$; Address Space $n_i \supseteq n_j$; Action $a_i \neq a_j$
Relation	Address Space $n_i \not\subset n_j \wedge n_j \not\subset n_i \wedge n_i \cap n_j \neq \phi$ Agreement $\rho_i = \rho_j$;Action $a_i \neq a_j$
overlap	Address Space $n_i \not\subset n_j \wedge n_j \not\subset n_i \wedge n_i \cap n_j \neq \phi$ Agreement $\rho_i = \rho_j$; Action $a_i = a_j$
Squamous overlap	Only layer 3 header field is used as condition; only layer 2 header field is used as decision condition; only layer 4 header field is used as condition

2) *Conflict control method*

At present, the strategy conflict control method is divided into open-loop control method and closed-loop control method. The closed-loop control method is based on the concept of feedback loop. There are several measures for closed-loop control: (1) monitoring the network system to detect when and where conflicts occur. (2) The conflict information is transmitted to the network security application layer. (3) The administrator adjusts the network system traffic resources to solve the conflict. The disadvantage of the solution to the conflict of the closed-loop control strategy is that it is adjusted after the event. When the policies are deployed, multiple security policies act on the network at the same time, and the network performance deteriorates due to policy conflicts in the process of operation, the closed-loop control will work. The disadvantage is that conflict prevention cannot be realized.

The open-loop control method is to consider the factors related to policy conflict before issuing the security strategy and traffic traction strategy, so as to avoid policy conflict when the network is working. PGA (policy graph abstraction) [7] is an automatic intention driven mechanism for mapping traffic to VSFS. It uses graph structure to detect policy conflicts and achieve conflict resolution. PGA allows network policies to be represented as graph structures. Multi-entity such as users, administrators and tenants can write policies independently, and submit policies through PGA user interface (UI), which can combine the policies specified by high-level into low-level configuration rules, solving the problem of automatic expression, conflict free and fast combination of network policies.

In our system, PGA function is placed in the security policy management module and traffic traction policy management module. The demand service function chain provided by PGA architecture has the following functions: each policy maker is allowed to independently specify the function of service chain policy; SSFC has the function of immediate policy combination to meet the combination requirements of a single policy; the framework must be automatic and have no ambiguity for network traffic [8].

PGA only focuses on the detection and coordination of policies before they are deployed, and does not focus on the conflict detection of running state. It belongs to the open-loop control strategy conflict method. Under the SDN architecture, the underlying network and policy implementation are transparent to the application layer users. When making network policy, they only need to care about the policy making. PGA supports the conflict detection and coordination of various strategies such as SSFC. In the data test of large-scale enterprise network, PGA shows good data processing ability and good delay, which verifies the feasibility of PGA[9].

I. *Virtual Security Function Manager(VSFM)*

The virtual security function manager is mainly responsible for the resource and life cycle management of the virtual security function (VSFS). It monitors the status of each virtual security function, creates its own resources, expands and shrinks its capacity. VNFM manages VSFS based on VSF description.

J. *Virtual Security Infrastructure Manager(VSIM)*

Virtual security infrastructure (VSI) includes the virtualization layer (hypervisor or container management system, such as docker, and Vswitch) and physical resources, such as servers, storage devices, switches and other three kinds of hardware resources: computing, storage, and networks. It is a resource that undertakes the tasks of computing, storage, internal and external interconnection and interworking.

VSI can be deployed across several physical locations. VSI is a general virtualization layer. All physical resources are virtualized into a unified shared virtual resource pool. These resources are transparent for running VSFS on it[10]. The main function of VSIM is to manage and monitor the whole infrastructure resources (including hardware resources and virtual resources).

K. *Virtual Security Function Orchestrator(VSFO)*

The main function of virtual security function Orchestrator is to create virtual network and network security service, monitor virtual network security service, choreograph virtual network security function topology, VSFs and overall resource management, which is the control core of the whole SDS architecture.Its main functions are as follows: NSVO generates security service function chain (SSFC) by arranging different virtual network functions (VSFS), manages the life cycle of security service function chain, coordinates the life cycle of VSFS with the support of VSFM, coordinates the management of various resources with the support of VSIM, and manages VSFS and network Network function virtualization infrastructure (NSVI) resource association and mapping relationship, to ensure that the required resources and connections are optimized [11].

L. *Application Layer*

Under the SDN network architecture, the network model has changed from a host centric model to a data centric model. Higher flexibility is required for cloud computing, big data center network, and network function deployment model of cloud architecture. Solution: the security control layer provides programming interface for application layer users, so that users can control the network. The network service provider must be able to provide virtual network function (VNFs), and present flexible, agile, dynamic and scalable network function visualization (NFV) technical service delivery for application layer[12]. In NFV environment, administrators deal with various services, specify service policies for subscribers of each network application function, and migrate application workload.

III. SYSTEM SECURITY ANALYSIS

TABLE II. SECURITY ISSUES RELATED TO DIFFERENT PARTS OF THE SYSTEM

Affected parts Type of attack		App layer	Virtual switch routing manager	Safety diversion control platform	Virtual security Orchestrator / Manager	Cloud diversion virtual machine	Security resource pool
Unauthorized access	Unauthorized controller access			√			√
	Unauthorized application	√					
Data leakage	Flow rule discovery				√		
	Forwarding channel discovery				√		
Tampering data	Tampering with flow rules			√			
Malicious application	Spoofing rule insertion	√					
	Controller hijack		√		√		
Denial of service	Flood attack of interactive computer in control layer					√	√
	switcher flow table flood attack		√				
Configuration problem	Lack of TLS					√	√
	Policy execution issues	√		√	√		

We end up with security issues related to different parts of the system, as shown in TABLEⅡ. Suppose our system includes P vulnerable components, $p = 1,2,3,\ldots\ldots N$ The vulnerable points on each vulnerable component are expressed as : $V_p: = \{v_{p,1}, v_{p,2}, \ldots\ldots, v_{p,np}\}$ Every weakness is easy to be exploited by attackers to attack the system. Each set of vulnerabilities is known to attackers and defenders. Each tenant configures its own server system on the cloud operating system by using the app of the application layer, which will produce one or more vulnerabilities.

The configuration of a user on P vulnerable components is described as $C_p:\{c_{p,1}, c_{p,2}, \ldots\ldots, c_{p,m_p}\}$ We use function mapping π_p to associate each system configuration with the set of vulnerability points, which is expressed as $\pi_p : C_i \rightarrow 2^{v_p}$

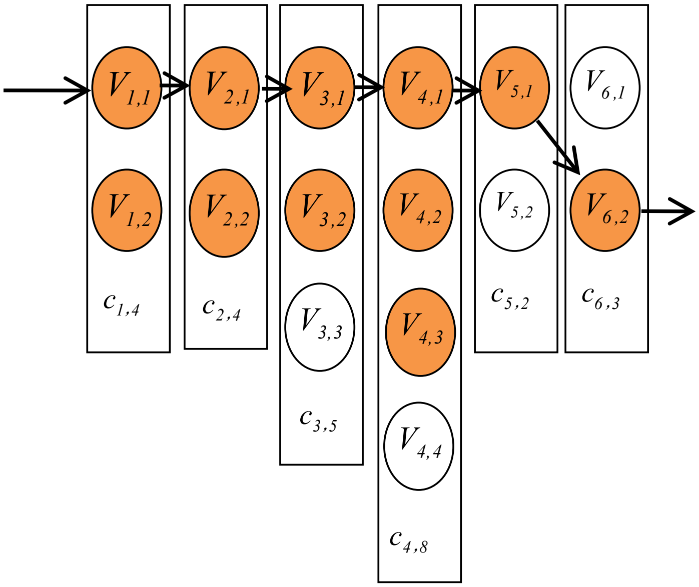

Figure 2. Configuration and attack propagation sequence

In Figure 2 there are six vulnerable components: $p = 1,2,3,4,5,6$ Each vulnerable component has two to four vulnerabilities. There are four possible flexible configurations for vulnerable component 1 $C_1 = \{c_{1,1}, c_{1,2}, c_{1,3}, c_{1,4}\}$ As shown in Figure 2, the configuration scheme we choose is $c_{1,4}$ that it exposes two system vulnerabilities to attackers, $\pi_1(c_{1,4}) = \{v_{1,1}, v_{1,2}\}$. For the same reason: $\pi_2(c_{2,4}) = \{v_{2,1}, v_{2,2}\}$, $\pi_3(c_{3,5}) = \{v_{3,1}, v_{3,2}\}$, $\pi_4(c_{4,8}) = \{v_{4,1}, v_{4,2}, v_{4,3}\}$, $\pi_5(c_{5,2}) = \{v_{5,1}\}$, $\pi_6(c_{6,3}) = \{v_{6,2}\}$

In the configuration scheme $\{c_{1,4}, c_{2,4}, c_{3,5}, c_{4,8}, c_{5,2}, c_{6,3}\}$,Attackers can launch a successful attack through a series of mining, such as $\{v_{1,1}, v_{2,1}, v_{3,1}, v_{4,1}, v_{5,1}, v_{6,2}\}$.

If the system configuration scheme remains static, the attacker will launch a planned and organized system scan and vulnerability mining against the configuration scheme until a successful attack on the system. To avoid the above, the defender can change the configuration scheme, such as changing $c_{1,4}$ to $c_{1,3}$,changing $c_{2,4}$ to $c_{2,3}$, changing the whole system configuration series to $\{c_{1,3}, c_{2,3}, c_{3,4}, c_{4,5}, c_{5,3}, c_{6,2}\}$ .In this way, the attacker's attack plan based on the original network configuration will fail under the new configuration. The system realizes that the defender can randomly configure all vulnerable components in the system to resist multi-level attacks.

IV. Summary

As the author of reference[5] said, software defined security is just a kind of thinking. When we analyze the different implementations of different SDS products, we should not delve into the details, and should just think about "how to improve the overall security protection efficiency of this architecture".

The author thinks that many domestic and foreign manufacturers have launched their own SDS products, and we need an open platform similar to the network security operating system. This paper is a small attempt in this direction.

Acknowledgment

First of all, We want to thank all the authors of the references. It is because of their hard work that We can stand on the shoulders of giants and move on. Secondly, we would like to thank all the companies that provide the experimental environment and data for this article. Finally, we would like to thank the editors of this book for their meticulous and valuable comments, so that this article can meet the readers.

2019 GuangDong Seedling Project.No2019-SY07

2019 Natural Science Foundation Project of GuangDong foundation and applied basic research foundation (general project) No 2019A1515011841

References

[1] Zhang Chaokun, Cui Yong, Tang HeYi,Wu JianPing," State-of-the-Art Survey on Software-Defined Networking (SDN)" Journal of software， vol.26(1), pp. 62-81, 2015.

[2] Izzat Alsmadi, Dianxiang Xu, "Security of Software Defifined Networks: A Survey", Computers & Security, vol.53, pp.79‑108, 2015

[3] Green Alliance Technology, "Green Alliance Technology software definition security white paper [D]", Green Alliance Technology, 2016

[4] "Huawei SDN industry chain", Baidu Library, 2014, https://wenku.baidu.com/view/b685f421e45c3b3566ec8b50.html

[5] Alireza Shameli Sendi, Yosr Jarraya, Makan Pourzandi, Mohamed Cheriet, “Effificient Provisioning of Security Service Function Chaining Using Network Security Defense Patterns”, IEEE Transactions on Services Computing, 2016.

[6] Peng Daqin, Lai Xiangwu, Liu Yanlin, “Multi path routing algorithm for fat tree data center network based on SDN “, Computer Engineering, vol.44 (4), pp. 41-45, 65,2018.

[7] Chaithan Prakash, Jeongkeun Lee, Yoshio Turner, Joon-Myung Kang, Aditya Akella, Sujata Banerjee, Charles Clark, Yadi Ma, Puneet Sharma, Ying Zhang. “Pga: Using graphs to express and automatically reconcile network policies”, ACM SIGCOMM Computer Communication Review, vol. 45, pp.29‐42., 2015.

[8] Zhou Tongqing, Cai Zhiping, Xia Jing, Xu Ming. “Traffic engineering based on software defined network”, Journal of software., vol.27 (2), pp.394-417 ,2016.

[9] Wu Quanfeng, Chen Ming, Xing Changyou, et al, “Design and implementation of a stream access security system based on Sdn “, Journal of Jiangsu University (NATURAL SCIENCE EDITION), vol. 37 (2), pp.201-208, 2016.

[10] Li Zhaobin, Li Weilong, Wei zhanzhen, Liu Mengtian., “Research and implementation of key modules of SDN data security processing mechanism”, Computer application., vol.38 (7), pp. 1929-1935,2018.

[11] Zuo Qingyun, Chen Ming, Zhao Guangsong, et al, “SDN technology research based on openflow”, Journal of software, vol.24 (5), pp.1078-1097, 2013.

[12] Ankur Chowdhary, Sandeep Pisharody, Dijiang Huang, “SDN Based Scalable MTD Solution in Cloud Network”, In Proceedings of the 2016 ACM Workshop on Moving Target Defense, pp. 27‐36., ACM. 2016.